2015

Towards dynamic adaption of user's organisational information security behaviour

Mutlaq Alotaibi
Centre for Security, Communications and Network Research, Plymouth University

Steven Furnell
Centre for Security, Communications and Network Research, Plymouth University, Security Research Institute, Edith Cowan University

Nathan Clarke
Centre for Security, Communications and Network Research, Plymouth University, Security Research Institute, Edith Cowan University

DOI: 10.4225/75/57b698e1d9389
13th Australian Information Security Management Conference, held from the 30 November – 2 December, 2015 (pp. 28-36), Edith Cowan University Joondalup Campus, Perth, Western Australia.

TOWARDS DYNAMIC ADAPTION OF USER'S ORGANISATIONAL INFORMATION SECURITY BEHAVIOUR

Mutlaq Alotaibi[1], Steven Furnell[1,2] and Nathan Clarke[1,2]
[1]Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK
[2]Security Research Institute, Edith Cowan University, Perth, Australia
{Mutlaq.Alotaibi, S.Furnell, N.Clarke}@plymouth.ac.uk

Abstract
The weakest link in the field of information security that has been identified in the literature is the organisation's employees. Information security policy compliance is one of the main challenges facing organisations today. Although implementing technical and procedural measures clearly helps to improve an organisation's information security, the human factor or the employees' compliance with these measures is the key to success. However, organisations are now having some issues regarding the extent of employee adherence to policy. The problem of employees being unaware or ignorant of their responsibilities in relation to information security is still an open issue. The proposed idea in this paper will seek to enhance end user adherence to information security policies by proposing a framework for security policy compliance monitoring and targeted awareness raising. The foremost aim of this framework is to increase users' awareness of the importance of following information security policies. Continuously subjecting users to targeted awareness and monitoring their adherence to information security policies should enhance the effectiveness of such awareness efforts. The proposed framework is a part of on-going research and is intended to provide a foundation for future research on a dynamic adaption of users' behaviour with information security policies.

Keywords
Information security management, Information security awareness, information security policy, Targeted awareness.

INTRODUCTION
Many researchers have identified computer end users as the weakest link in the information security chain (Bashorun et al. 2013; Veiga & Eloff 2010). Therefore, information security policy is considered to be the cornerstone of information security management and an organizational approach that mitigates potential threats from employees. In the workplace, all employees should be made aware of acceptable and unacceptable user behaviour and the first step to achieving this is to implement a proper formal information security policy. Knapp et al. (2009) stated that organizations must realize that having policies, processes and procedures is as important as having a firewall, an intrusion detection system, a virtual private network (VPN) or any other technical solution. Security policy is defined in a formal document that addresses acceptable and unacceptable behaviour of users in relation to dealing with information assets in a secure manner. It is part of a formal information security control and a baseline statement of the information security tasks which should be followed by the employees. According to SANS (2014), a security policy is typically "a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area".

It is necessary to implement different forms of protection of a physical, logical and procedural nature. A wide variety of security policies have been established and implemented in different organizations. Basically, an information security policy is divided into two main categories: a high level security policy and a lower level security policy (Baskerville & Siponen 2002). Firstly, the high-level policy reflects security concerns and objectives at highest level of abstraction. For example, the organization states the significance of information resources, and defines personal or management responsible for securing this resource. Secondly, the lower-level policies follow a high level policy as a response to the identified risks reflecting the organization objectives, or addressing specific countermeasures. An example of lower-level information security policy is, when employees are asked to change their password every 90 days. Thus, an organization should have a high-level security policy, which provides the guiding context within which other lower level policies would reside.

Non-compliant employees or those who are unaware of information security policy have become a major concern to organisations since they pose a threat to the computing environment security. In Ernst and Young (EY's) global information security survey results (2013), 57% of the surveyed organisations considered their

employees to be the biggest threat to information security, whilst 38% indicated that unaware or careless employees pose the greatest threat. Moreover, According to Price Waterhouse Coopers (PwC) 70% of organisations where security policy was poorly understood had staff-related breaches, whereas only 41% of organisations where the policy was well understood had the same (PwC 2014).

Apparently, in order to strengthen the human factor, which is the weakest link in the security chain, more consideration should be given to information security awareness. Actually, 72% of large and 63% of organisations have provided on-going security awareness training for their staff (PwC 2015). However, the problem of employees being unaware of their responsibilities in relation to information security is still an open issue. Despite the presence of the best information security awareness programmes, obstacles exist that make the successful implementation of awareness activities more challenging. These common obstacles (ENISA 2010; Qudaih et al., 2014) are: 1) Implementation of new technology. 2) One size fits all. 3) Too much information. 4) Lack of organisation. 5) Failure to follow up. 6) No explanation of why.

This paper builds upon existing Literature on information security policies and related issues, with a view of dynamic adaption of security awareness. The paper then explores the proposed dynamic adaption of user's organizational information security behaviour framework. A detailed discussion and outline of the future work is subsequently presented.

THE CURRENT EXTENT OF USE OF INFORMATION SECURITY POLICY

An information security breaches survey conducted by (PriceWaterhouseCoopers PwC 2014) implied that most large organizations now implement their own documented security policy (as illustrated in Table 1). More encouragingly, the information security policy adoption level within small businesses increased from 54% in 2013 to 60% in 2014. Another survey conducted by E&Y Global Information Security (2013) reported that information security policies were owned at the highest organizational level in 70% of all organizations. Apparently, this result is a good indication that the majority of organizations are aware of the importance of information security policy.

However, having such a policy in place is not a guarantee that employees will adopt the required behaviour; they may not behave as they are expected to due to a lack of understanding of the policy's content. Essentially, in the aforementioned survey PwC (2014), approximately 25% of the respondents believed that their members of staff understood their policies well, while approximately 20% of the respondents believed that their staff's level of understanding of their security policies was poor. In spite of the great effort made by many organisations to promote information security awareness, most employees are still unaware of security requirements. This claim is strongly supported by the PwC (2015) report, which indicates that 75% of large organisations suffered a staff-related breach and nearly 31% of small organisations had a similar occurrence.

Table 1 reveals some consolidated statistical information that explains the current extent of use of information security policy and the key policy-related issues. The information in this table was gathered mainly from two surveys performed by PWC and EY. They survey organizations across the world on areas concerning information security and breaches, and they usually produce a new survey report every year.

Table 1: Summary of information security policy usage and key policy-related issues

Items / **Source**	Security Policy implementation	Threats by employees	Security awareness promotion
The E&Y Global Information Security (EY Global information 2013)	70 % of all organizations indicated that information security policies were owned at the highest organizational level.	25% of organizations indicated that careless or unaware employees increase in past 12 months.	Security awareness and training was mature in 30% of organizations, undeveloped in 41% and non-existent in 29%.

Information Security Breaches Survey (PriceWaterhouseCoopers PwC 2015)	98% of large organisations and 60% of small organisations have a documented information security policy	75% of large organisations suffered a staff-related breach and nearly 31% of small organisations had a similar occurrence. 72% of companies where the security policy was poorly understood had staff related breaches.	For large organisations, on-going security training has increased up to 72% , and for small organisations, up to 72%

The key findings from the above table, nearly all large organizations now have a formally documented information security policy, whereas more than half of small organizations have implemented the same. However, roughly more than half of organizations consider their employees to be a major threat to their information security, and almost a third of them view careless or unaware employees as the most likely threat. Employee's good understanding of security policy positively affects the overall security of an organization. This is seen in PwC (2014) where 72% of organizations where the security policy was poorly understood had staff related breaches. According to security awareness efforts, only around half of organizations provide their staff with continuous awareness and training activities.

KEY SECURITY POLICY RELATED ISSUES AND CHALLENGES

Nowadays, organizations continue to face challenges in relation to encouraging user adherence to implemented security policy, for instance Internet usage policy (Saran and Zavarsky 2009). Many tools and methods have been used to increase the compliance of end users, such as user signed policies, monitoring tools, logon pop-ups, website restrictions and disciplinary action. However, the effectiveness of such information security policy is still threatened by some challenges. Many security researchers have attributed these challenges (Silowash et al. 2012; Economist Intelligence Unit (EIU) 2009; PwC 2014; Prince 2014; Saran & Zavarsky 2009; Kirlappos et al. 2015; Veiga & Eloff 2009) , as explained in the following subsections. Figure 1 gives an overview of these challenges, which associated with security policies.

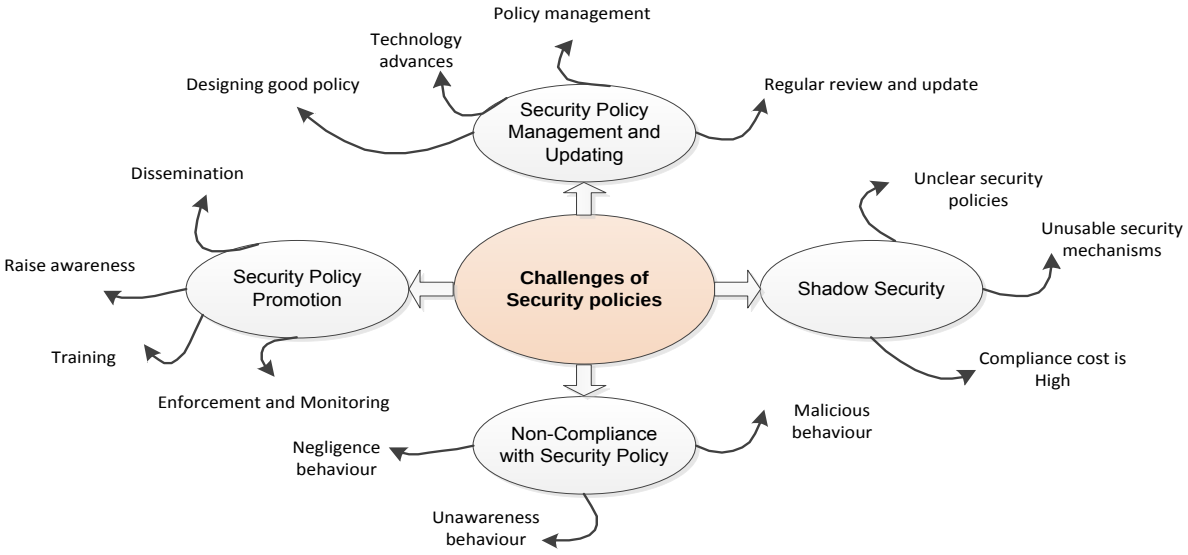

Figure 1: Information Security Policy Challenges

Security Policy Management and Updating

Usually, security solutions, such as security policy, procedures, controls and training, are neglected by many organizations, not being continuously reviewed or even updated (Colwill 2009). According to Silowash et al. (2012), organizations may face challenges when attempting to implement best practice in relation to information security, as follows:

- Designing good policy: It can be a challenge for many organizations to create an information security policy that covers all the significant issues, such as flexibility, fairness, legislation and fit to the organization.
- Policy management: Organizations must consistently review and update policies to ensure that they are still meeting all the organization's needs and ensure that updates are disseminated to all employees.

Security Policy Promotion

The implementation of a good information security policy will not be effective unless there is a comprehensive plan to promote it and raise awareness of it among employees. Hence, organizations should be encouraged to promote, communicate, enforce and maintain information security policy.

However, organizations face challenges associated with the promotion and dissemination of their information security policies. In the Economist Intelligence Unit survey (EIU 2009), most of the IT managers claimed that information security policies had been developed by their organizations to overcome many concerns, for example, use of Personal Computers (PCs), applications and websites. However, only a few of these organizations had seriously instilled this culture into their employees. This is supported by PwC (2014), who state that:

"Although there are more written policies in place to guide employees' behaviours towards security, we haven't yet seen this translate into better understanding of these policies".

Non-Compliance with Security Policy

Non-compliance with information security policy is primarily considered to be a human problem rather than a technical issue, for example a lack of security tools. Therefore, the main solutions are possibly non-technical, for example awareness and training, and these can obviously contribute to mitigating the potential threats from non-compliant users.

A study conducted by Saran and Zavarsky (2009) upon approximately 2000 employees in an insurance company found that even if a policy is re-released for the staff to sign or a reminder pop-up or email is sent to them, they may not engage with the policy since they can sign without reading or just ignore the pop-up or email. Hence, educating and training staff about policy is crucial if non-compliance is to be eliminated. Wilson (2010) stated that users tend to dislike the active controls that are imposed on their PCs, and this is commonly seen in many organizations. The reason for hating these controls is due to them being a group of no commands (e.g. no Google apps, no Facebook, no Skype, etc.). He also added that in reality, users tend to find a way around these controls to do what they want to do. Therefore, it is better to convince users to use policies and to enforce them firmly

Shadow Security

Traditionally, organizations manage the security of their information assets via mechanisms and a security policy that employees are expected to comply with. There are two main categories regarding the expected behaviour of employees in relation to such security policies: compliance and non-compliance.

However, a third type of employee security policy behaviour has been identified: shadow security (Kirlappos et al. 2015). Shadow security is defined by Kirlappos et al. (2014) as "employees going around IT to get the IT services they want on their own". In other words, employees implement their own security solutions when they believe that compliance is beyond their capacity or will affect their productivity. For example, when an organization creates and implements a strong password security policy, such as 12 characters in length and a combination of upper letters and symbols, some employees will find it difficult to remember the password. Employees in this case will comply with the policy but play around with it by writing the password on a note and putting it under the keyboard. In the aforementioned example, an employee is considered to be complaint with password policy; however, there is also a shadow security policy, and this may threaten an organization's security.

USER BEHAVIOUR WITH INFORMATION SECURITY POLICY

In the IS field, the human factor is the vulnerability considered to be the most unpredictable one. In addition, the human factor is characterized by being the most variable and thus the hardest to control. When organizations deal with the human factor, the procedure for placing staff with the right level of commitment to the policies of Information technology (IT) should contain an assessment of the security behaviour of individual members of staff. A number of studies have suggested that when the level of compliance with and acceptance of the established security polices and controls amongst the members of staff in an organization is measured, the success of those policies can be anticipated. Members of staff can show different levels of compliance. Furnell & Thomson (2009) name eight levels of compliance, starting with 'culture' and ending with 'disobedience'.

- Culture (compliance): Security is a natural party of users' daily behaviour.
- Commitment (compliance): Security is not part of the natural behaviour of users, but if they are given enough guidance and shown leadership, they will acknowledge the need and make an effort to comply.
- Obedience (compliance): Users need to be given instructions rather than just guidance and leadership in order to comply.
- Awareness (compliance): Users are aware of security but are not fully complying and not showing the required behaviour.
- Ignorance (non-compliance): Users are unaware of security issues at this level and represent a higher risk of accidental adverse effects.
- Apathy (non-compliance): Users are aware of the role they should play at this level but are not willing to show compliance as part of their behaviour.
- Resistance (non-compliance): Users are aware of the role they are expected to play in security but are working against the aspects of the required practices they do not agree with.
- Disobedience (non-compliance): Users intentionally break the rules and deliberately fail to comply with security and its established controls.

Violation of IS policies is associated with intentional behaviour, malicious intention or non-malicious intention. Firstly, intentional behaviour that leads to non-compliance with information security policy is due to the malice of the user. Thus, the user intentionally does not adhere to the information security policy of his or her organization in order to cause damage. Secondly, not all intentional behaviour that leads to non-compliance is considered to be malicious. An example of this is a user intentionally violating an implemented information security policy due to a lack of awareness or even carelessness. Users whose unintentional behaviour leads to non-compliance may not be aware of security policies. Therefore, there are three main reasons for users unintentionally violating IS policy: awareness, negligence and errors.

Hence, there is a need for an effective solution that dynamically addressing all the potential behaviours of employees dealing with their security policies in order to monitor and raise their awareness. Moreover, finding a way to target the right employees at the right time is still a problem that needs to be solved. In the following, we will define and explain a framework that is intended to mitigate the issue.

DYNAMIC ADAPTION OF USER'S ORGANISATIONAL INFORMATION SECURITY BEHAVIOUR FRAMWORK

Usually, Information security policies are promoted through traditional information security awareness methods, although these delivery methods have some shortcomings in their effectiveness as mentioned earlier. Moreover, the successful implementation of such security policies can face from some obstacles and challenges, which also has been discussed previously. As a solution, the dynamic adaption of users organizational information security behaviour framework has been proposed.

In figure 2, the framework is designed to emphasize the significance of delivering an effective awareness method to the end users. The framework mainly concentrates on three major issues: information security policies, security behaviour (security events) and the awareness engine. It seeks to continuously monitor users' behaviour in relation to such information security policies and raise compliance levels. Therefore by subjecting user to continuous and targeted awareness, the level of user's compliance would raise. The framework will provide information about users' behaviour by using security monitoring tools. This information will then be aggregated and classified to ascertain whether or not there is any non-compliant behaviour.The main aim of the compliance and awareness engine in this framework is to persuade users to comply or to continue to comply if they are already doing so. Thus, each user will be subjected to targeted awareness if he or she does not comply. Moreover, the engine will investigate the factors that influence each user's behaviour in order to facilitate the awareness process. A points system will also be used to reward or punish users in order to motivate them.

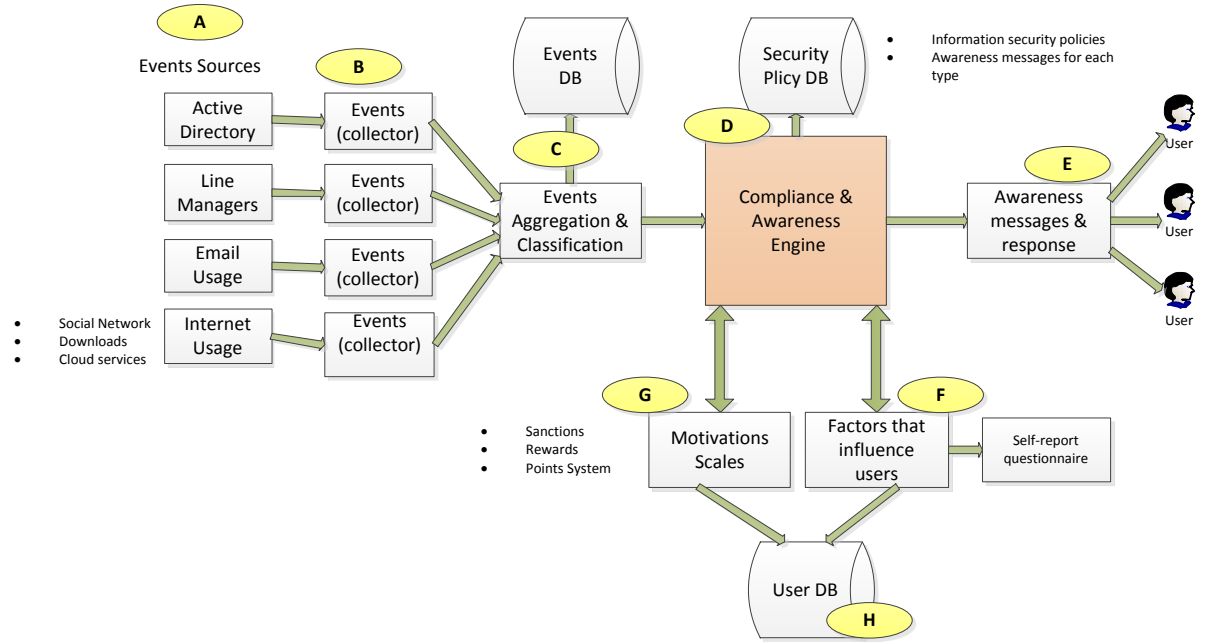

Figure 2: Security Policy Compliance Monitoring and Targeted Awareness Raising Framework

The framework will focus mainly on three aspects, as listed below and then described in the paragraphs that follow (matching the labels used in the Figure):

- Events (user behaviour with security policy): The behaviour monitoring
- Information Security policies
- Awareness raising and promotion targeted awareness and monitoring

Events sources (labelled as A in the framework), Security events (or the possible violation of security policy) will be collected via two methods: from security monitoring and control devices and applications; and manually from security reports or line managers. The events sources may include but are not limited to:

- Active directory: Active directory is a database that keeps track of all the user accounts and passwords in an organisation..
- Line managers: here the input will come manually from managers, who report any behaviour that does not comply with the information security policy, such as when a user writes down his or her password or leaves the computer unlocked.
- Email usage: rather than raising awareness about email usage for all employees, the framework will focus only on employees who are using email as a part of their daily work.

Internet usage: many organisations believe that threats coming from the Internet are the biggest concern. When employees use social networks, downloads and cloud storage services without complying with the security policy that has been specifically created for Internet usage, there is a potential threat to an organisation. In this case, the framework will send awareness messages to the employees based on their Internet usage. For example, the user who accesses any type of cloud storage services will need targeted awareness about the security policy relevant to this type of usage.
The most important part of the framework is the security awareness engine (lablled as D in the framwork), where security events will be analysed and the causal factors will be identified. Therefore, this part of the framework will use an event to increase awareness. For example, if a particular user violates the policy on Internet usage, this event will be analysed and the causal factors will be identified. As a result, the form of persuasive technology best suited to this incident will be used to improve the awareness of the particular user of the specific aspect of Internet usage policy. Thus, the main objectives of using persuasive computing technology are the individualisation and personalisation of awareness raising. The following are some points that will be covered:

- There will be targeted awareness for each employee.
- Something has happened. What should be done about it?
- It is essential to have a personalised persuasive profile regarding what motivates different users.

- The use of persuasive technology in motivation behaviour change has recently gained the attention of many researchers as it is a useful approach to promoting behaviour change, and it is now being applied in many domains, such as marketing, health and psychology.
- Personalising persuasive strategies. Each user will be given targeted security awareness based on their behaviour (events), and the awareness type will focus mainly on the part of the security policy that they have violated rather than on all the security policy.
- There will be a database containing information on security policies and the awareness messages for each type of breach of the security policy.

The following Table 2 gives an overview of the rest of the framework components :

Table 2: Framework Elements Description

Labelled as	Elements	Description
B	Events collection	The aim of this process is to collect data about employees within the computing environment from many sources, such as Web gateway, active directory, SIEM, network traffic and auditing tools.
C	Events classification	Events will be classified based on the information security type and storage in the events database. Therefore, prior to storing events in the database, they will be put through a process that aims to classify each one based on certain norms, such as type, number, user id, security policy id and department.
E	Awareness messages	The awareness messages will be taken from the security policy Database (DB) based on the events type and the user ID so that the user will receive a series of awareness messages about the security policy that is not clear to them and which they may have violated. Therefore, here the persuasive computing technique will be used to enhance user awareness of the organisation's IS policy or, in other words, to promote the security policy
F	Factors that influence users	This process will aim to identify the factors (organisational or human) that may impact upon employee behaviour in relation to the security policy. Here, an electronic questionnaire may be utilised to investigate such factors.
G	Motivation scales	Rewards and sanctions will be used as motivation and deterrence, respectively. Here, a points system will be used, whereby employee who comply and shows good behaviour will be given points and noncompliance will result in minus points.
H	User database	Each user will have a profile, the main aim of which will be to record users' awareness history. This may include some useful information about employees such as security events or behaviour, factors that influence users, awareness or persuasion messages that have been sent, points and the behaviour after the awareness raising efforts

Practically, the framework will be implemented by collecting data about each user separately. Then this information will be process over the framework to enhance user compliance. For example, the password policy for network users is may be set via the Active Directory side. Therefore, organisations often advise their employees to change passwords every two or three months without enforcing this policy electronically through Active Directory options because it will be a headache to enforce this policy. In this scenario the framework will try to monitor those who have not changed their password for a long period of time and send them a targeted awareness message. Before sending the message, the awareness engine in the framework will investigate the factors that influence users and then the suitable persuasive messages will be sent. Moreover, the motivation scale will be used in this case so the compliant user is granted some points as rewards in contrast to the incompliant user, who will be punished. Another example would be unattended workstation (PCs), whereby any user who left his or her computer unlocked would be targeted in order to increase the awareness of this issue. Therefore, the framework will get these events information about idle PCs from Win32 API (Application programing interface).

CONCLUSION AND FUTURE WORK

The foremost aim of this framework is to increase users' awareness of the importance of following information security policies. Continuously subjecting users to targeted awareness and dynamically monitoring their adherence to information security policies should enhance the effectiveness of such awareness efforts. The novelty of the proposed framework depends upon three significant aspects: monitoring, persuasion and the influencing factors upon users. Therefore, all of these aspects will be utilized in order to enhance the awareness of end users. However, further research is required in order to better understand of the effectiveness of the proposed solution and the extent of users' acceptance of it. Moreover, the proposed framework may have some limitation in terms of covering all information security policies, such asa physical security policy.

REFERENCES

Bashorun, A., Woewui, A. & Parker, D., 2013. Information security: To determine its level of awareness in an organization. In *In 2013 7th International Conference on Application of Information and Communication Technologies*. Ieee, pp. 1–5. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6722704.

Baskerville, R. & Siponen, M., 2002. An information security meta-policy for emergent organizations. *Logistics Information Management*, 15(5/6), pp.337–346.

Colwill, C., 2009. Human factors in information security: The insider threat – Who can you trust these days? In *Information Security Technical Report*. Elsevier Ltd, pp. 186–196. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1363412710000051 [Accessed September 8, 2014].

EIU, 2009. *Power to the people? Managing technology democracy in the workplace*, Available at: http://graphics.eiu.com/marketing/pdf/Technology Democracy.pdf. [Accessed April 10, 2015].

EY Global information, 2013. *Under cyber attack EY ' s Global Information Security Survey 2013*, Available at: http://www.ey.com/Publication/vwLUAssets/EY_-_2013_Global_Information_Security_Survey/$FILE/EY-GISS-Under-cyber-attack.pdf. [Accessed April 10, 2015].

Furnell, S. & Thomson, K.-L., 2009. From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud & Security*, 2009(2), pp.5–10. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1361372309700193 [Accessed October 23, 2014].

Kirlappos, I., Parkin, S. & Sasse, M.A., 2015. " Shadow Security " as a tool for the learning organization. In SIGCAS Computer & Society, pp. 29–37.

Kirlappos, I., Parkin, S. & Sasse, M.A., 2014. Learning from "Shadow Security" : Why understanding non-compliant behaviors provides the basis for effective security.

Knapp, K.J. et al., 2009. Information security policy: An organizational-level process model. In *Computers & Security*. pp. 493–508. Available at: http://www.sciencedirect.com/science/article/B6V8G-4WSHK03-2/2/65673d7d064cc45cd182b82622c6acda.

PriceWaterhouseCoopers PwC, 2015. *INFORMATION SECURITY BREACHES SURVEY*, Available at: http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf. [Accessed April 10, 2015].

PriceWaterhouseCoopers PwC, 2014. *INFORMATION SECURITY BREACHES SURVEY 2014*, Available at: https://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf. [Accessed April 10, 2015].

Prince, P., 2014. More Than Half of Enterprise Employees Receive No Security Training: Survey Finds. *security week*. Available at: http://www.securityweek.com/more-half-enterprise-employees-receive-no-security-training-survey-finds [Accessed May 1, 2015].

Qudaih, H. a et al., 2014. Security Awareness in an Organization. *Persuasive Technology Contributions Toward Enhance Information Security Awareness in an Organization*, 10(4), pp.180–186.

SANS, 2014. Information Security Policy Templates. Available at: http://www.sans.org/security-resources/policies/general [Accessed May 15, 2015].

Saran, M. & Zavarsky, P., 2009. A Study of the Methods for Improving Internet Usage Policy Compliance. In *2009 International Conference on Computational Science and Engineering*. Ieee, pp. 371–378. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5283299 [Accessed October 24, 2014].

Silowash, G., Cappelli, D. & Moore, A., 2012. *Common Sense Guide to Mitigating Insider Threats 4th Edition*, Available at: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA585500 [Accessed January 21, 2015].

The European Network and Information Security Agency (ENISA), 2010. *The new users ' guide :How to raise information security awareness*, Available at: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide.

Veiga, a. & Eloff, J.H.P., 2010. A framework and assessment instrument for information security culture. In *Computers & Security*. Elsevier Ltd, pp. 196–207. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167404809000923 [Accessed September 20, 2014].

Wilson, T., 2010. Why Employees Break Security Policy (And What You Can Do About It). Available at: http://www.darkreading.com/risk/why-employees-break-security-policy-(and-what-you-can-do-about-it)/d/d-id/1133433 [Accessed April 10, 2015].